USDA PRIVACY IMPACT ASSESSMENT FORM

Agency: Departmental Administration

System Name: Enterprise Physical Access Control System (ePACS)

System Type:
- ☒ **Major Application**
- ☐ **General Support System**
- ☐ **Non-major Application**

System Categorization (per FIPS 199):
- ☐ **High**
- ☒ **Moderate**
- ☐ **Low**

Description of the System:
ePACS is the physical access component of the Department's Homeland Security Presidential Directive 12 (HSPD-12) and FIPS 201, Personal Identity Verification (PIV) compliance effort. ePACS will provide the Department a means to centralize and distribute physical access control data related to the PIV-II credentialed individuals to all USDA agency Physical Access Control Systems (PACS).

ePACS will integrate data from the Office of Chief Information Officer (OCIO), Enterprise Identity Management System (EIMS) and will also integrate with other USDA enterprise systems for human resources (EMPowHR) and payroll and personnel.

Who owns this system? (Name, agency, contact information**)**
Name: Russ Ashworth
Title: Director
Office: Departmental Administration, Office of Security Services
Address: USDA South Building
1400 Independence Avenue, Suite 1456
Washington DC, 20250
Phone: 202-720-3937
Email: Russ.Ashworth@usda.gov

Who is the security contact for this system? (Name, agency, contact information**)**
Name: Nic Afshartoos
Title: Information System Security Program Manager
Office: Departmental Administration, Office of Chief Information Officer
Address: Reporters Building
300 7th Street SW, Suite 0034
Washington DC, 20024
Phone: 202-720-8466
Email: Nic.Afshartoos@usda.gov

Who completed this document? (Name, agency, contact information**)**

Name: Mike Defrancisco
Title: Deputy Chief Physical Security
Office: Departmental Administration, Office of Security Services
Address: Reporters Building
300 7th Street SW, Suite 101
Washington DC, 20024
Phone: 202-401-0665
Email: Mike.Defrancisco@usda.gov

DOES THE SYSTEM CONTAIN INFORMATION ABOUT INDIVIDUALS IN AN IDENTIFIABLE FORM?

Indicate whether the following types of personal data are present in the system

QUESTION 1 Does the system contain any of the following type of data as it relates to individual:	Citizens	Employees
Name	**No**	**Yes**
Social Security Number	**No**	**No**
Telephone Number	**No**	**No**
Email address	**No**	**No**
Street address	**No**	**No**
Financial data	**No**	**No**
Health data	**No**	**No**
Biometric data	**No**	**Yes**
QUESTION 2 Can individuals be uniquely identified using personal information such as a combination of gender, race, birth date, geographic indicator, biometric data, etc.? NOTE: 87% of the US population can be uniquely identified with a combination of gender, birth date and five digit zip code[1]	**No**	**Yes**
Are social security numbers embedded in any field?	**No**	**No**
Is any portion of a social security numbers used?	**No**	**No**
Are social security numbers extracted from any other source (i.e. system, paper, etc.)?	**No**	**No**

If all of the answers in Questions 1 and 2 are NO,
You do not need to complete a Privacy Impact Assessment for this system and the answer to OMB A-11, Planning, Budgeting, Acquisition and Management of Capital Assets, Part 7, Section E, Question 8c is:
3. No, because the system does not contain, process, or transmit personal identifying information.

If any answer in Questions 1 and 2 is YES, provide complete answers to all questions below.

[1] Comments of Latanya Sweeney, Ph.D., Director, Laboratory for International Data Privacy Assistant Professor of Computer Science and of Public Policy Carnegie Mellon University To the Department of Health and Human Services On "Standards of Privacy of Individually Identifiable Health Information". 26 April 2002.

DATA COLLECTION

3. Generally describe the data to be used in the system.

Security Management Information including physical access card status, category, expiration date, card holder emergency response responsibilities.

Personal Identity and Logistic information such as: First Name, Last Name, Middle Name, Agency, Department, Office Address, City, State, Zip, Phone, Federal Agency Smart Credential Number (FASCN),

4. Is the use of the data both relevant and necessary to the purpose for which the system is being designed? In other words, the data is absolutely needed and has significant and demonstrable bearing on the system's purpose as required by statute or by Executive order of the President.

☒ Yes
☐ No

5. Sources of the data in the system.
5.1. What data is being collected from the customer?

None

5.2. What USDA agencies are providing data for use in the system?
USDA OCIO specifically and all other USDA Agencies

5.3. What state and local agencies are providing data for use in the system?

None

5.4. From what other third party sources is data being collected?
None

6. Will data be collected from sources outside your agency? For example, customers, USDA sources (i.e. NFC, RD, etc.) or Non-USDA sources.

☒ Yes
☐ No. If NO, go to question 7

6.1. How will the data collected from customers be verified for accuracy, relevance, timeliness, and completeness?

N/A

6.2. How will the data collected from USDA sources be verified for accuracy, relevance, timeliness, and completeness?

Automated referential integrity checks and business rules will be performed on the data before it is collected from the other sources. Additional referential integrity checks and business rules will be performed on the data in a staging server before being transferred into ePACS. Data integrity reviews based on a 95% confidence interval on the entire ePACS record population will be performed on a recurring basis.

6.3. How will the data collected from non-USDA sources be verified for accuracy, relevance, timeliness, and completeness?

N/A

DATA USE

7. Individuals must be informed in writing of the principal purpose of the information being collected from them. What is the principal purpose of the data being collected?

Homeland Security Presidential Directive for Personally Identity Verification

8. Will the data be used for any other purpose?

☐ Yes
☒ No. If NO, go to question 9

8.1. What are the other purposes?

9. Is the use of the data both relevant and necessary to the purpose for which the system is being designed? In other words, the data is absolutely needed and has significant and demonstrable bearing on the system's purpose as required by statute or by Executive order of the President

☒ Yes
☐ No

10. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected (i.e. aggregating farm loans by zip codes in which only one farm exists.)?

☐ Yes
☒ No. If NO, go to question 11

10.1. Will the new data be placed in the individual's record (customer or employee)?

☒ Yes
☐ No

10.2. Can the system make determinations about customers or employees that would not be possible without the new data?

☐ Yes
☒ No

10.3. How will the new data be verified for relevance and accuracy?

Automated referential integrity checks and business rules will be performed in data prior to import or integration into the system.

11. Individuals must be informed in writing of the routine uses of the information being collected from them. What are the intended routine uses of the data being collected?

Physical access control, personal identity verification and overall security management.

12. Will the data be used for any other uses (routine or otherwise)?

☐ Yes
☒ No. If NO, go to question 13

12.1. What are the other uses?

13. Automation of systems can lead to the consolidation of data – bringing data from multiple sources into one central location/system – and consolidation of administrative controls. When administrative controls are consolidated, they should be evaluated so that all necessary privacy controls remain in place to the degree necessary to continue to control access to and use of the data. Is data being consolidated?

☐ Yes
☒ No. If NO, go to question 14

13.1. What controls are in place to protect the data and prevent unauthorized access?

The system has been categorized as a High impact system and subject to 17 families of controls identified in the baseline security requirements of Annex 3 of NIST SP 800-53, Recommended Security Controls for Federal Information Systems.

Among the controls employed are: separation of duties, mandatory access controls, encryption of data at rest, in process and in transmission. Other controls include: appropriate disposal of data output and encryption of backup and recovery media.

14. Are processes being consolidated?

☒ Yes
☐ No. If NO, go to question 15

14.1. What controls are in place to protect the data and prevent unauthorized access?

At this time, the system is in the development phase of its life cycle, minimum baseline security controls based on an approved security categorization will be implemented and the system certified and accredited before going into production. In depth will be performed to ensure that the risk of unauthorized access is at an acceptable level.

DATA RETENTION

15. Is the data periodically purged from the system?

☐ Yes
☒ No. If NO, go to question 16

15.1. How long is the data retained whether it is on paper, electronically, in the system or in a backup?

15.2. What are the procedures for purging the data at the end of the retention period?

15.3. Where are these procedures documented?

16. While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?

Changes to the data must be approved and in the system within 16 hours

17. Is the data retained in the system the minimum necessary for the proper performance of a documented agency function?

☒ Yes
☐ No

DATA SHARING

18. Will other agencies share data or have access to data in this system (i.e. international, federal, state, local, other, etc.)?

☐ Yes
☒ No. If NO, go to question 19

18.1. How will the data be used by the other agency?

18.2. Who is responsible for assuring the other agency properly uses of the data?

19. Is the data transmitted to another agency or an independent site?

☐ Yes
☒ No. If NO, go to question 20

19.1. Is there the appropriate agreement in place to document the interconnection and that the PII and/or Privacy Act data is appropriately protected?

20. Is the system operated in more than one site?

☒ Yes
☐ No. If NO, go to question 21

20.1. How will consistent use of the system and data be maintained in all sites?

Robust configuration management and database mirroring will ensure that consistent use of the system and data is maintained in all sites.

DATA ACCESS

21. Who will have access to the data in the system (i.e. users, managers, system administrators, developers, etc.)?

Only authorized USDA managers, employees and contractors will have access to the data in the system

22. How will user access to the data be determined?

Formal access control and personnel security policies will be written as part of the baseline security requirements. Moreover, a position sensitivity matrix will be developed and continually maintained to determine whether access is required and the appropriate level of access if it is deemed necessary.

22.1. Are criteria, procedures, controls, and responsibilities regarding user access documented?

☒ Yes
☐ No

23. How will user access to the data be restricted?

The principle of least privilege is employed on this system. User's access will be restricted based on user role. Only an Administrator would have access to all data. An extremely restricted number of administrators will be designated.

23.1. Are procedures in place to detect or deter browsing or unauthorized user access?

☒ Yes
☐ No

24. Does the system employ security controls to make information unusable to unauthorized individuals (i.e. encryption, strong authentication procedures, etc.)?

☒ Yes
☐ No

CUSTOMER PROTECTION

25. Who will be responsible for protecting the privacy rights of the customers and employees affected by the interface (i.e. office, person, departmental position, etc.)?

The system security organization consisting of the Agency Privacy Officer, Designated Approving Authority, Certifying Authority, Information System Security Program Manager and System Owner.

26. How can customers and employees contact the office or person responsible for protecting their privacy rights?

The person responsible for protecting their privacy rights can be contacted by telephone or e-mail.

27. A "breach" refers to a situation where data and/or information assets are unduly exposed. Is a breach notification policy in place for this system?

☒ Yes. If YES, go to question 28
☐ No

27.1. If NO, please enter the POAM number with the estimated completion date:

28. Consider the following:

- Consolidation and linkage of files and systems
- Derivation of data
- Accelerated information processing and decision making
- Use of new technologies

Is there a potential to deprive a customer of due process rights (fundamental rules of fairness)?

☐ Yes
☒ No. If NO, go to question 29

28.1. Explain how this will be mitigated?

29. How will the system and its use ensure equitable treatment of customers?

The system will allow for due process and comply with the American Disabilities Act (ADA) for Section 508 Compliance

30. Is there any possibility of treating customers or employees differently based upon their individual or group characteristics?

☐ Yes
☒ No. If NO, go to question 31

30.1. Explain

SYSTEM OF RECORD

31. Can the data be retrieved by a personal identifier? In other words, does the system actually retrieve data by the name of an individual or by some other unique number, symbol, or identifying attribute of the individual?

☒ Yes
☐ No. If NO, go to question 32

31.1. How will the data be retrieved? In other words, what is the identifying attribute (i.e. employee number, social security number, etc.)?

The data can be retrieved by last name and Federal Agency Smart Credential Number (FASCN).

31.2. Under which Systems of Record notice (SOR) does the system operate? Provide number, name and publication date. (SORs can be viewed at www.access.GPO.gov)

ePACS anticipates that will operate under its own system of records unless otherwise directed.

31.3. If the system is being modified, will the SOR require amendment or revision?

N/A

TECHNOLOGY

32. Is the system using technologies in ways not previously employed by the agency (e.g. Caller-ID)?

☐ Yes
☒ No. If NO, the questionnaire is complete.

32.1. How does the use of this technology affect customer privacy?

The system will not affect customer privacy.

Upon completion of this Privacy Impact Assessment for this system, the answer to OMB A-11, Planning, Budgeting, Acquisition and Management of Capital Assets, Part 7, Section E, Question 8c is:

1. Yes.

PLEASE SUBMIT A COPY TO
THE OFFICE OF THE ASSOCIATE CHIEF INFORMATION OFFICE/CYBER SECURITY

Privacy Impact Assessment Authorization Memorandum

I have carefully assessed the Privacy Impact Assessment for the

_____

(System Name)

This document has been completed in accordance with the requirements of the EGovernment Act of 2002.

We fully accept the changes as needed improvements and authorize initiation of work to proceed. Based on our authority and judgment, the continued operation of this system is authorized.

_____ _____

System Manager/Owner
OR Project Representative
OR Program/Office Head.

Date

_____ _____

Agency's Chief FOIA officer
OR Senior Official for Privacy
OR Designated privacy person

Date

_____ _____

Agency OCIO

Date